PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of Defense Component:

US Army Chief Information Officer

2. Name of Information Technology System:

Army Knowledge Online (AKO)

3. Budget System Identification Number (SNAP-IT Initiative Number):

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):

2611

5. IT Investment (OMB Circular A-11) Unique Identifier (from IT-43/FOIT Database -- if applicable):

N/A

6. Privacy Act System of Records Notice Identifier:

AO025-1 CIO G6 Army Knowledge Online (AKO) Information System Records (January 9, 2007, 72 FR 956).

7. OMB Information Collection Requirement Number and Expiration Date:

N/A

8. Type of authority to collect information (statutory or otherwise):

10 U.S.C. 3013, Secretary of the Army;
Department of Defense Directive 8500.1, Information Assurance (IA);
DoD Instruction 8500.2, Information Assurance Implementation;
AR 25-1, Army Knowledge Management and Information Technology;
Army Regulation 25-2, Information Assurance; and
E.O. 9397(SSN)

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

The purpose of AKO is to perform knowledge management and register users in order to facilitate electronic communications and collaboration among DoD personnel and other

authorized guest users. This system serves as an Army controlled repository for information needed by DoD personnel necessary for performance of duties and other DoD-related functions. AKO serves as host for numerous Army applications and provides protection for those applications through role-based access. Access is controlled based on individual needs for specific types of information to perform official duties. Statistical data, with all personal identifiers removed, may be used by management for system efficiency, workload calculation or reporting purposes. AKO also provides electronic communications within the military community.

10. Identifiable Information to be Collected, its Nature and Source:

The AKO Liteweight Directory Access Protocol Data Store (LDAP) & Electronic Data Dictionary (EDD) includes the following primary personal information: individual's name, operator's/user's identification, SSN, birth date, email address, organization or home address, duty or home telephone and fax numbers, military and civilian rank/grade, military branch, military occupational specialty (MOS), assigned password, account types, experience, skills, and unstructured text entered at user discretion which may or may not contain PII. Army program managers may post documents to AKO that contain PII from various Army programs and functionalities depending on the subject matter. The source of this information is directly from system users, individual record subjects, Army activities and program managers and Army personnel database systems.

11. Method of Information Collection:

Information is collected in automated form and remains in an automated environment that system users can access. In support of Defense Knowledge Online (DKO), information is also collected from other databases by data transfer from authoritative sources such as Defense Eligibility Enrollment Registration System, Integrated Total Army Personnel Database and Defense Manpower Data Center for non-Army personnel.

12. Purpose of Collection and How Identifiable Information/Data will be used:

AKO collects data to verify an individual's eligibility for registration, continued authority to use the system, authentication of identity, access control and general identification management. The system develops a user directory to facilitate contact, to broadcast information and to share information with other registered users. This system serves as an Army controlled repository for information needed by DoD personnel for performance of duties and other DoD-related functions.

13. Does system create new data about individuals through aggregation?

This system does not create new personally identifiable data about individuals through aggregation.

14. Internal and External Information/Data Sharing:

Data will be shared among Agency personnel, authenticated users and portal administrators. Internal DoD agencies that would obtain access to PII in this system, on

request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Criminal Investigative Service, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

15. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses and how consent is granted:

A Privacy Act statement describing the use, dissemination and collection of information in identifiable form is located on the website at the registration portal and each time the user logs on to the system. System use and registration are voluntary, and individuals choose to enter their own PII.

16. Information Provided to the Individual, the Format, and the Means of Delivery:

A Privacy Act statement describing the use, dissemination and collection of information in identifiable form is located on the website at the registration portal and each time the user logs on to the system. System use and registration are voluntary, and individuals choose to enter their own PII.

17. Describe the administrative/business, physical, and technical processes and data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

The users include Active Duty Military, Federal Civil Service personnel and authorized contractors who have a need to know in order to perform official government duties. There is limited system access and use for members of the extended military community. Both contractor and government employees may have access requirements and are limited to specific or general information in the computing environment based on need to know. The System Administrator defines specific access requirements dependent upon each user's role. Each specific application in the system may further restrict access via application-unique permission controls. Currently, only system users and service liaisons and their authorized contract users have the capability to connect to the system. Information is made available to users through the application or Enterprise server. Each authorized user must enter an appropriate User/Identification and Password before being authorized access to the resources. There is daily monitoring, daily notification of inactive accounts, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). Files transferred across the Internet are encrypted.

18. Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures:

Appropriate safeguards are in place for the collection, use, and sharing of information.

Security measures are adequate and the risk to AKO is minimal. Information is protected by user passwords, firewalls, antivirus software, and Common Access Card access. Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals.

19. Classification and Publication of Privacy Impact Assessment:

The system is unclassified but contains sensitive privacy act data. The PIA may be published in full.